U.S. Department of Justice

Operation Web Snare

A Joint Law Enforcement Initiative

August 26, 2004

Web Snare

Executive Summary:

Operation Web Snare represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Web Snare exemplify the growing volume and character of Cyber crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue Cyber criminals, both domestically and abroad. Focused efforts to pursue Cyber criminals internationally, has led to the development of enhanced proactive capabilities in several countries, and numerous investigative successes highlighted within this initiative. The development of international resources is closely coordinated with the DOJ, the U.S State Department and a growing list of E-Commerce industry partners.

Criminal schemes included in this initiative include: criminal spam, phishing, spoofed or hijacked accounts, international re-shipping schemes, Cyber-extortion, auction fraud, credit card fraud, Intellectual Property Rights (IPR), Computer Intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of "traditional crimes" that continue to migrate on-line.

The substantial accomplishments captured in this initiative are attributable to the growing number of joint Cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state, and local agencies. Substantial industry partnerships developed in coordination with associations such as the Direct Marketing Association (DMA), the Merchants Risk Council (MRC), the Business Software Alliance (BSA), and the Software and Information Industry Association (SIIA) also contributed significantly to the success of this initiative. Operation Web Snare has been coordinated at the Federal level with the Department of Justice, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), the U.S Postal Inspection Service, the U.S. Secret Service, the Federal Trade Commission, and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State and Local participation in this effort was amplified in coordination with The National White Collar Crime Center (NW3C).

Operation Web Snare includes more than 160 investigations, in which more than 150,000 victims lost more than $215 million dollars. Through these investigations more than 350 subjects were targeted, resulting in 150 arrests/convictions, 117 indictments, and the execution of more than 170 search/seizure warrants. Although significant in number,

these investigations represent only a fraction of the Cyber crime problem, underscoring not only the need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well.

Potential Nexus to Terrorism:

In today's global economy, the financial critical infrastructure community has become more and more dependent on the Internet, as communications and financial transactions have rapidly transitioned to this medium. Terrorists and their support groups, like any organized criminal enterprise, have increasingly availed themselves of the resources and perceived anonymity associated with the Internet. From the 19 September 11th terrorists, to the recent subjects arrested in Europe, such groups have demonstrated an increasing use of the internet to communicate, generate funds and develop resources in support of terrorism. National Security Advisor, Condoleezza Rice noted, after the events of Sept 11th and in support of the Patriot Act that, "Terrorism is inexorably woven through the Internet."

In a recent statement posted on an Islamic Fundamentalist website (azzam.com) the author stated, **"'We strongly urge Muslim Internet professionals to spread and disseminate news and information about the jihad through e-mail lists, discussion groups and their own Web sites. The more Web sites, the better it is for us. We must make the Internet our tool."**

The FBI through the IC3 has noted an increase in on-line complaints where illegally obtained funds have been identified as flowing to parts of the world where such groups have been known to operate. Cyber crime schemes generating these funds include Phishing/Identity Theft, as well as numerous credit card schemes, auction fraud, and advanced fee scams. The FBI will continue to coordinate the development of leads/investigations having such a nexus with representatives of the Intelligence community and the Department of Homeland Security.

Common Cyber Crime Schemes

Spoofing/Phishing

Spoofing and Phishing (pronounced "fishing") are somewhat synonymous in that they refer to forged or faked electronic documents. Spoofing generally refers to the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual sender. Phishing, often utilized in conjunction with spoofed e-mail, is the creation of a Web site to make that site appear as the legitimate business website. Once the fraudulent website has been launched, the spoofed Web sites attempt to dupe the unsuspecting victims into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim usually traverses to the spoofed website via a hyperlink that was provided to him/her in a spoofed e-mail.

Spam

The illegal distribution of unsolicited bulk e-mail.

Advance-Fee Fraud Schemes

The victim is required to pay significant fees in advance of receiving a substantial amount of money or merchandise. The fees are usually passed off as taxes, or processing fees, or charges for notarized documents. The victim pays these fees and receives nothing in return. Perhaps the most common example of this type of fraud occurs when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe he has won a large award in a nonexistent foreign lottery.

Business/Employment Schemes

Typically incorporate identity theft, freight forwarding, and counterfeit check schemes. The fraudster posts a help-wanted ad on popular Internet job search sites. Respondents are required to fill out an application wherein they divulge sensitive personal information, such as their date of birth and Social Security number. The fraudster uses that information to purchase merchandise on credit. The merchandise is sent to another respondent who has been hired as a freight forwarder by the fraudster. The merchandise is then reshipped out of the country. The fraudster, who has represented himself as a foreign company, then pays the freight forwarder with a counterfeit check containing a significant overage amount. The overage is wired back to the fraudster, usually in a foreign country, before the fraud is discovered.

Counterfeit Check Schemes

A counterfeit or fraudulent cashier’s check or corporate check is utilized to pay for merchandise. Often these checks are made out for a substantially larger amount than the purchase price. The victims are instructed to deposit the check and return the overage amount, usually by wire transfer, to a foreign country. Because banks may release funds from a cashier's check before the check actually clears, the victim believes the check has cleared and wires the money as instructed. One popular variation of this scam involves the purchase of automobiles listed for sale in various Internet classified advertisements. The sellers are contacted about purchasing the autos and shipping them to a foreign country. The buyer, or person acting on behalf of a buyer, then sends the seller a cashier's check for an amount several thousand dollars over the price of the vehicle. The seller is directed to deposit the check and wire the excess back to the buyer so they can pay the shipping charges. Once the money is sent, the buyer typically comes up with an excuse for canceling the purchase, and attempts to have the rest of the money returned. Although the seller does not lose the vehicle, he is typically held responsible by his bank for depositing a counterfeit check.

Credit/Debit Card Fraud

Is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured Web sites, or can be obtained in an identity theft scheme.

Freight Forwarding/Reshipping

The receiving and subsequent reshipping of on-line ordered merchandise to locations usually abroad. Individuals are often solicited to participate in this activity in chat rooms, or through Internet job postings. Unbeknownst to the reshipper, the merchandise has been paid for with fraudulent credit cards.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

Investment Fraud

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

OPERATION WEB SNARE

This map depicts the locations of the investigative actions highlighted in Operation WEB SNARE:

SLAM-Spam:

The SLAM-Spam initiative is an ongoing sub-project within Operation Web-Snare and represents one of the first true Public/Private Alliances developed jointly between law enforcement and industry to specifically target a growing crime problem. This initiative was developed through the Internet Crime Complaint Center (IC3), in conjunction with industry, coordinated through the Direct Marketing Association (DMA). This initiative began in the fall of 2003, with the development of two jointly staffed teams of analysts and investigators. One Team continues to focus on the methods or techniques utilized by spammers, while the other targets the fundamentally criminal schemes victims were invited to participate in through the unsolicited "SPAM" e-mail they received. This project continues to be advanced in coordination with law enforcement, industry and our partners at the Federal Trade Commission. This initiative was designed to identify and develop cases, as well as trends/techniques that should be considered as part of the investigative strategy, and training for investigators & analysts involved in cyber crime matters. Various successful investigations included in Operation Web-Snare were substantially developed or advanced through this project.

Sampling of Investigations from Operation Web Snare

The following cases are a sampling of the investigations that are a part of this initiative. Some of the information contained herein has been generalized due to the on-going nature of the investigations:

Spam

On July 28, 2004, in an FTC civil action, the defendants agreed to an injunction against use of the "Windows Messenger Service," part of the Microsoft Windows operating system, to barrage consumers' computers with pop-up ads for the pop-up blocking software they sold. The FTC alleged that the defendants' pop-up ads appeared as frequently as every ten minutes in the forefront of consumers' screens, caused consumers to lose data and work productivity, caused applications to freeze, and caused some computers to crash.

Spam/Spoofing/Computer Intrusion/Extortion

Myron Tereshchuk, 42, of Hyattsville, Maryland, pled guilty to attempting to extort $17 million over the Internet. For more than a year, Tereshchuk harassed a patent firm. The defendant sent the victim firm's clients hundreds of e-mails, many of which were "spoofed" to resemble the firm's authentic correspondence. The e-mails contained statements derogatory to the victim company, attached sexually explicit patent applications, and disclosed documents that were believed to have been proprietary in nature. Tereshchuk obtained the confidential information by gaining unauthorized access to the victim firm's computer network and by searching through the company's trash, which was awaiting collection by a shredding company. The defendant sent his extortion demands virtually anonymously by using equipment from his automobile to gain unauthorized access to unsecured wireless computer networks in residences and businesses in Maryland and Virginia.

Tereshchuk demanded $17 million, threatening to disclose additional proprietary patent information and launch distributed denial-of-service attacks, if his demands were not met. Using innovative surveillance techniques, the FBI was able to catch the defendant in the act of sending extortion e-mails to the victim. At the time of the defendant's arrest, he was in possession of his laptop, an antenna, and other computer equipment which could be used to access unsecured wireless networks. Tereshchuk is awaiting sentencing, which has been set for October 22, 2004. He faces a maximum potential sentence of 20 years imprisonment and a $250,000 fine.

Phishing

In June of 2004, the FBI received notification from Microsoft Inc (MSN) that an individual was sending spam e-mails to a number of MSN's customers. These e-mails were sent from a spoofed e-mail address, billing@msn.com, to make it appear to the recipients that the e-mail they had received was a legitimate communication from MSN.

The e-mail advised the recipients to update their financial account records with MSN by clicking on a hyperlink within the e-mail, which would allegedly direct the user to a secure website where payment information could be updated and verified for accuracy. A copy of the e-mail is depicted below:

----- Original Message ----**From:**
billing@msn.com **Subject:** MSN
Billing Update

> *Dear MSN Customer,*
>
> *We regret to inform you that technical difficulties arose with the installation of new software upgrades. Unfortunately part of our customer database, and backup system became inactive. In order to enjoy your MSN experience and keep your account active, we will require you to enter your information in our online billing center at your convenience or calling our customer support team (1-877-676-3678). The average hold time is 45 minutes.*
>
> *As an added incentive to using the web based account center we offer 50% credit to your next bill. Please take a moment and re-enter your account information at our secure online account center by visiting:*
> *http://billing.msn.com@msn6.dr.ag*
>
> *Sincerely,*
> *Sandy Page*
> *MSN Billing Department*

When the recipients clicked on the hyperlink located within the spammed e-mail, they were taken to a web page designed to look like an authentic MSN web page. Investigation determined that when customers submitted their financial information to this fraudulent site, the information was directed not to MSN, but to an e-mail address allegedly created by the subject of this investigation to harvest personal financial information provided by his unwitting victims.

The screen shot depicted below is an image of the fraudulent phishing web page to which users were directed upon clicking on the hypertext in the spoofed e-mail.

Investigators traced the internet protocol (IP) addresses used in launching this phishing attack to Internet Service Providers (ISP) located in the United States, India, and to a free and fully automatic redirect service located in Austria. The use of multiple ISPs, redirect services, free and unverified e-mail accounts, and compromised computers, often located in multiple countries, are typical of the techniques employed by criminals launching phishing attacks, as a means of obfuscating their true identities and locations. Analysis of available computer log files in this case determined that the subject of this investigation was actually operating from a computer located in the United States. In July 2004, a federal search warrant was executed by the FBI at the subject's Iowa residence.

Phishing

The FTC settled cases against two participants in a phishing scheme designed to trick consumers into providing confidential financial information under the belief that the defendants were an "AOL Billing Center." The second defendant, sued in the Eastern District of New York, is an unidentified minor. Both defendants are barred for life from sending spam. One defendant faces criminal charges. The case was brought with the invaluable assistance of the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section, Federal Bureau of Investigation's Washington Field

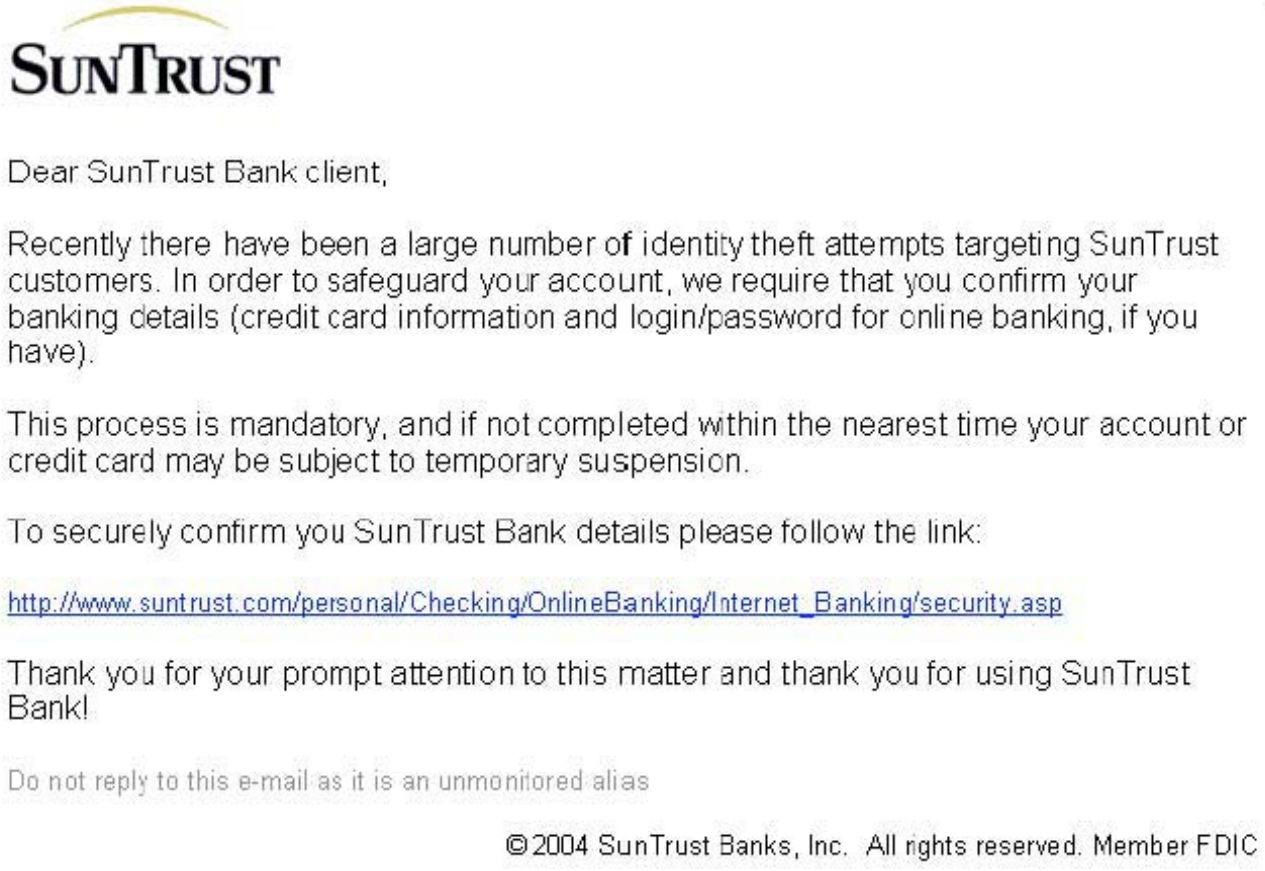
Office, and United States Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad.

Phishing Trends Associated with Spam Cases:

Recently the Internet Crime Complaint Center (IC3) has seen a new breed of Phishing scams being advertised in spam e-mails. Old Phishing scams would reconstruct a look-alike site for whoever they were trying to impersonate. If they were trying to target eBay users by claiming they needed to update their personal information, for example, the phishers would use all of the images and formatting associated with a legitimate eBay page, to attempt to make their fraudulent web pages/emails look authentic. The phishing page would be located on the phisher's site. It would collect all of the information from the victims; e-mail that data to an email address controlled by the phisher, and then redirect the victim to the actual site being impersonated. By redirecting to the real site at the end, the victim would be more likely to believe that the whole thing was legitimate.

Although the IC3 still receives reports of phishing scams like this, we have seen multiple new scams that use a very different technique. First of all, the e-mails advertising these scams put the body of the message into an image file, which makes filtering much more difficult. Secondly, the actual phishing site will use Javascript to open a new window in the foreground that harvests the victim's information, and will load the site being impersonated in the background to make the scam look even more authentic. Although these methods do not make tracking the scam any easier or harder, they are likely to fool more people into thinking that it is legitimate.

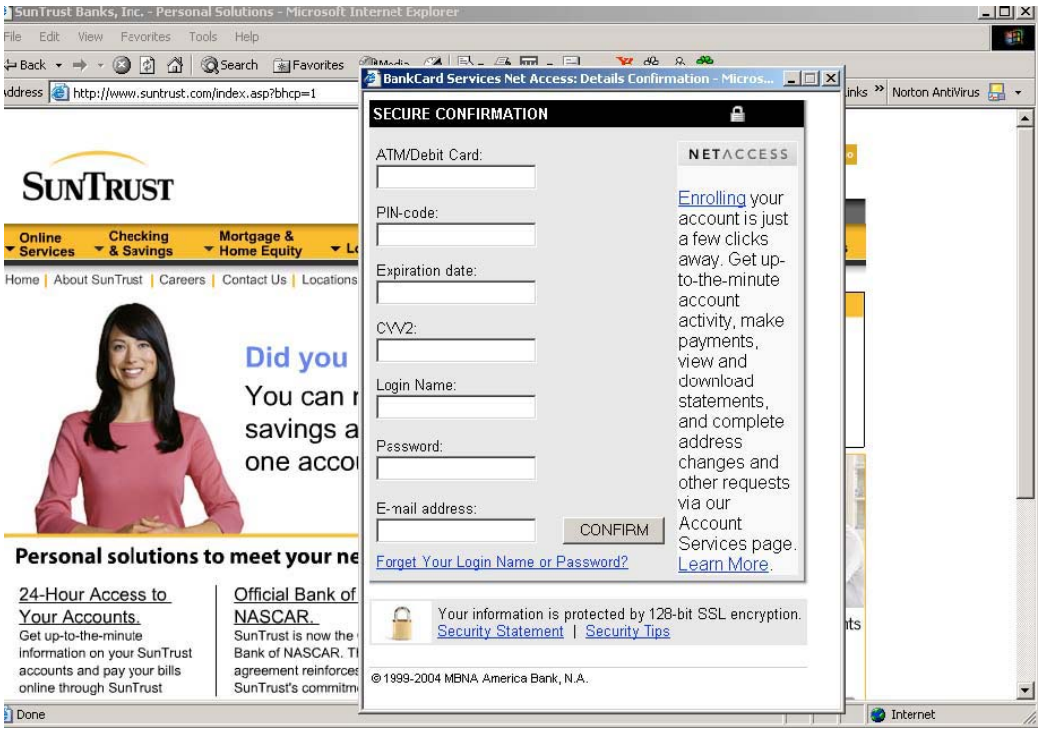
Another method used in the e-mail is to put the entire message into an image, and to put that image in the body of the e-mail. So the whole "Dear Mr. X, you need to update your account info" would be in an image file. This entire image is then covered with a clear image. Whenever the clear image is clicked on, it sends the user to the phishing page. A sample image is provided below:



If the victim clicks anywhere over the image in the e-mail, they are sent to the phishing page, because the entire image is overlapped with a transparent image that carries the link. The fact that all of the text is in an image means that it would be very difficult for an e-mail filter to process. The image is also typically followed by a long string of random characters to further confuse e-mail filters. The random characters, however, are written in a white font so they are not visible to the victim.

The Sites

The new trends discovered by the IC3, concerns the sites themselves providing a new pop-up window in the foreground, with a redirect of the background window to the legitimate impersonated website.



In the above screen capture, the phishing site was loaded, which popped up the "Secure confirmation" window and redirected the background window to SunTrust's real site. This makes it appear to the victim that SunTrust is really asking for the information, but the "Secure Confirmation" window is really being run off of the phishing site. When the victim enters their personnel information and clicks confirm, the information is sent to a script on the phishing site.

Phishing Party

During a "loud party" call, deputies of a local Sheriff's Department in Georgia quickly realized there was more going on at that location than just a party. Deputies noticed several laptops, numerous credit cards, and other indicia indicative of on-line criminal activity. Subsequently, a search warrant was obtained for the residence and the numerous laptops computers.

The subject was interviewed and admitted he was involved in deploying thousands of spam emails to unsuspecting recipients. The spammer explained, he utilized the spam email as his Phishing instrument for bank account information and credit card information (Identity Theft). The subject further explained that he would travel to the Atlanta metropolitan area, and locate an unsecured wireless network. Once located, he would launch his spam emails. The recipients of his spam emails were identified from the various email address listings he would purchase through on-line resources i.e. IRC rooms.

One of the subject's Phishing attempts provided him with credit card information for 18 accounts. He compromised those 18 accounts and the issuing bank incurred a loss

of $300,000. To help facilitate his criminal activity, the subject used seven vacant houses for his drop locations. The subject admitted that his on-line criminal activity has netted him approximately $75,000 to date. Investigation in this matter continues.

Election Fraud

The 161 member Firefighters Union in Odessa, Texas held an election for a position on the Board of Trustees which is responsible for the management of the Firefighters pension fund. Henry Guzman, a current member of the Board was running for reelection and had administrative access to the web server, located in California, which recorded the Union members votes. Guzman surreptitiously registered votes for himself using names and identification numbers of Firefighters. The fraud was discovered when a Firefighter logged into the system to vote and was given a message that he had already placed a vote.

On June 16, 2004 Guzman was indicted by a Federal Grand Jury on charges related to his unauthorized access to a computer system and the illicit votes he caused to be registered.

First Arrests Under New "CAN-SPAM" Legislation

Mark Sadek and Christopher Chung were arrested in April 2004, based upon a complaint charging them with violating the mail fraud and new anti-spam statutes after investigation revealed over 5.2 million recorded attempts by the defendants to send unsolicited emails through their system. The arrests marked the first time that the new anti-spam statute has been charged since the "CAN-SPAM Act" took effect on January 1, 2004. Daniel Lin and James Lin were also subsequently charged in the case.

During April and August 2004, search warrants were executed at: the defendants' business in West Bloomfield, Michigan; a Tampa, Florida computer facility; a New York Commercial Mail Receiving Agency; and a Canadian computer facility. The searches resulted in the seizure of numerous computers and other items deemed to be of evidentiary value.

The four defendants, operating under the business names Phoenix Avatar LLC and AIT Herbal Marketing, allegedly sold fraudulent medical products advertised via unsolicited e-mail, also known as "spam." The products were then shipped via the U.S. Mail. The CAN-SPAM Act prohibits misleading headers and other practices that conceal the origin of email ads.

The defendants allegedly would improperly access "open proxy" computers, which are computers with security flaws allowing anyone to transmit untraceable email. The defendants allegedly would use the open proxies to send "spam" containing advertisements for their fraudulent medical products. One such item was a purported diet patch that when applied to the skin caused significant weight loss without diet or exercise. This is an ongoing joint investigation being conducted by the U.S. Postal

Inspection Service and Federal Trade Commission.

Spam

The subject of this investigation, Howard Carmack, was sentenced by an Erie County, New York judge, to the maximum sentence of three-and-a-half to seven years in jail, after being convicted on New York State charges of all 14 counts facing him.

Carmack was found guilty of three counts of forgery, one count of criminal possession of a forgery device, five counts of identity theft, and five counts falsifying business records. These charges stemmed from Carmack's illegal activities in which he sent nearly 850 million spam e-mails through fraudulently registered Earthlink e-mail accounts which he had opened using stolen identities. Criminal charges in this case stemmed from an internal investigation launched by Earthlink investigators after they determined that a spam ring operating out of the Buffalo, New York, area was sending millions of spam e-mails, including advertisements for computer virus scripts, get-rich-quick schemes, work-at-home schemes, and body enhancement products. Earthlink's civil suit resulted in a $16.4 million judgment against Carmack for damages his spamming activity caused Earthlink, and a permanent injunction against any future spamming activity by Carmack. The Buffalo Cyber Task Force, composed of the FBI, the United States Secret Service, the Buffalo Police Department, the Erie County Sheriff's Office, the Greece Police Department, the New York State Attorney General's Office, and the New York State Police Department initiated a criminal investigation in May of 2003. During the execution of a federal search warrant, additional evidence of Carmack's illegal activities was obtained. Investigation determined that Carmack, using other individuals' identities, registered and operated 343 e-mail accounts from which he sent his spam. This case was prosecuted by the New York State Attorney General's Office, rather than in federal court, as Carmack's spamming activity occurred prior to the passage of the recently enacted CAN-SPAM legislation.

Spam

In June 2004, two defendants surrendered to Virginia law enforcement authorities following a five-count indictment for violating Virginia's law against sending illegal bulk e-mail, better known as "spam", via the Internet. The indictments allege that the defendants distributed a product known as Human Growth Hormones and knowingly contracted with illegal spammers to send bulk e-mail to unsuspecting recipients. They are accused of sending more than 10,000 illegal e-mails during a 24-hour period on specific dates in 2003 and 2004. They are also accused of falsifying or forging e-mail transmission, or other routing information known as the header, which prevents the recipient from knowing the true origin of the e-mail. The use of false information is what makes the act a crime, and the volume of e-mails sent elevates the charge to a felony. The

defendants face a maximum sentence of 25 years incarceration, if convicted on all counts. This case was investigated by the Commonwealth of Virginia's Attorney General Jerry W. Kilgore's Computer Crime Unit.

Spam

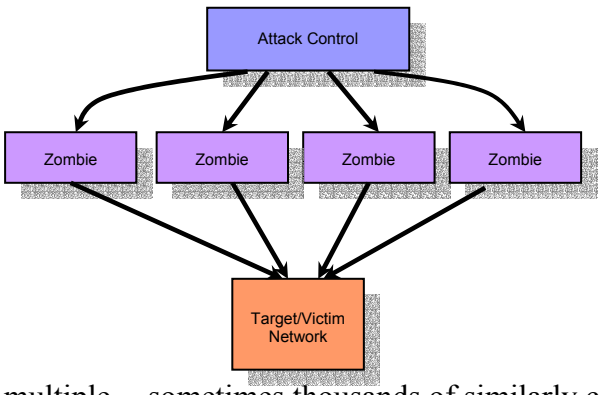
The FTC filed a complaint alleging that the defendants sent spam that deceptively promised a 2.95% or 3.0% mortgage when the advertised rates would be insufficient to pay interest due and would increase the consumer's loan balance. Defendants agreed to entry of a preliminary injunction pending trial on the FTC's charges.

Spam

On August 9, 2004, the U.S. Attorney's Office in Los Angeles also filed charges against a "wireless spammer" under the recently enacted CAN SPAM legislation as a result of an FBI investigation. Charges have been filed against Nicholas Tombros for sending spam e-mail messages advertising pornographic websites from his laptop computer while driving through suburbs of Los Angeles. Tombros used wireless antenna attached to his laptop and drove around the Los Angeles area to find open unencrypted wireless access points for computer networks. Tombros then gained access to the wireless networks and sent thousands of spam messages with advertising for pornography sites. Tombros is expected to appear in U.S. District Court on Monday, August 30 to face the federal charges.

Distributed Denial of Service Attack

A Distributed Denial-of-Service (DDoS) attack is one in which a multitude of compromised systems attack a single target, causing a sustained denial of service for users of the targeted system. The flood of incoming messages to the target computer system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks are extremely difficult or even impossible to counter once launched, and present an equally difficult task for law enforcement, since anonymity is an inherent feature of the DDoS attack and control systems.



A hacker begins a DDoS attack by exploiting vulnerability (often the vulnerability is the direct result of a virus or worm engineered for that purpose – often delivered via spam) in a computer system and making it the DDoS "master." From the master system (the Attack Control Mechanism in the graphic), the intruder identifies and communicates with multiple -- sometimes thousands of similarly compromised computers known as "zombies" or "bots" that are loaded with specialized attack software.

In the largest and first-ever case involving sophisticated denial of service attacks for commercial advantage, the U.S. Attorney's Office in Los Angeles has charged six men for launching crippling attacks against online competitors. Jay R. Echouafni, Chief Executive Officer of Orbit Communication Corporation in Massachusetts, was indicted by a federal grand jury yesterday on multiple charges of conspiracy and causing damage to protected computers after he and a business partner hired computer hackers to launch relentless distributed denial of service ("DDOS") attacks against Orbit Communication's online competitors. The indictment and a separate criminal complaint also filed yesterday allege that Echouafni and his business partner, Paul Ashley of Powell, Ohio, used the services of computer hackers in Arizona, Louisiana, Ohio and the United Kingdom to attack the Internet websites of RapidSatellite.Com, ExpertSatellite.Com and Weaknees.Com. The sustained attacks began in October 2003 and caused the victims to lose over $2 million in revenue and costs associated with responding to the attacks. In addition, the attacks also temporarily disrupted other sites hosted by the victims' Internet Service Providers including the United States Department of Homeland Security and Internet giant Amazon.Com.

The massive computer networks used to launch the DDOS attacks were created through the use of computer worms that proliferated throughout the Internet and compromised thousands of vulnerable computers. The infected computers, known as "Zombies," were then used by the co-conspirators to attack the victim computer systems by flooding the systems with massive amounts of data. This type of attack, once the domain of teenagers vying for attention, has become the tool of choice for tech-savvy and unscrupulous business owners attempting to sabotage competitors. Echouafni, depicted in the adjacent images, is a United States citizen originally from Morocco. He fled from the United States and is the target of an international manhunt led by the FBI. Operation Cyberslam was investigated by the FBI with the assistance of the London Metropolitan Police Service and the FBI Legal Attache in the United Kingdom. This matter is the first successful investigation of a large-scale DDoS network used for a commercial purpose in the United States.

Auction Fraud (Failure to Pay)

The subject of this investigation mailed checks written on closed or bogus bank accounts to numerous on-line auction sellers and mail order merchants across the United States and overseas. The worthless checks were sent as payment for merchandise the subject purchased over the Internet. In order to perpetrate the fraud, the subject opened boxes at commercial mail receiving agencies to receive the merchandise obtained with the worthless checks.

In June 2004, a federal grand jury in the Northern District of Texas returned an indictment charging the defendant with six counts of mail fraud. The defendant

voluntarily surrendered several items obtained with the worthless checks, including Baccarat crystal and a Rolex watch. To date, it is estimated over 500 victims were defrauded of more than $300,000. This case is being investigated by the United States Postal Inspection Service.

Lottery Scam

On June 30, 2004, the U.S. District Court for the District of Columbia entered a stipulated permanent injunction against operators of a "green card" lottery scam. The FTC alleged that the defendants had falsely represented that their Internet Web sites were affiliated with the U.S. government and could help consumers register for a permanent resident visa (green card). The order prohibits these practices and requires the defendants to pay $2.2 million in redress. The individual defendants have also pled guilty to federal criminal charges in connection with this scheme.

E-Commerce Fraud

The Federal Bureau of Investigation, along with the United States Attorney for the Southern District of Florida, the Internal Revenue Service, the U.S. Postal Inspection Service, and the Broward County Sheriff's Office indicted BERNARD ROEMMELE, SALVATORE ARGENTO, LESTER GILLESPIE, STEVE HEIN, and BEN TOBIN with crimes arising from their involvement in a complex Internet fraud and securities fraud scheme.

The indictment arose from the defendants' participation in promoting the fraudulent activities of CITX Corporation; formerly an internet service provider and alleged computer Technology Company, and its marketing partner PRSI, Inc. Through these companies, the defendants used the Internet to offer the public a non-existent e-commerce opportunity in exchange for $295 per person. Specifically, the offering promised customers an electronic website "store" which allegedly would provide customers with an opportunity to engage in e-commerce through electronically retailing goods and services on a pornography-free "Internet mall." Customers were falsely promised that they would earn commissions, not only from their personal sales, but also from the sales generated by the individuals whom they convinced to purchase these websites. In addition, the defendants used the Internet, false press releases, and other communications media to disseminate false and fraudulent information to corruptly induce individuals to purchase stock in CITX.

The indictment charges all defendants with one count of RICO conspiracy, one count of mail and wire fraud conspiracy and one count of money laundering conspiracy. In addition to those charges, defendant HEIN is charged with one count of obstruction of justice, and defendant ROEMMELE is charged with one count of securities fraud.

The Florida Attorney General's office initiated civil litigation against PRSI, and as a result of an ex parte filed by the Florida Attorney General's office, a receivership was appointed for the PRSI. PRSI has been closed down and the receiver has seized $4 million in assets. The criminal investigation has uncovered that over 45,000 people were

victimized throughout the course of the fraud schemes which involved criminal proceeds of over $15 million. This matter is one of the largest Internet fraud cases to be prosecuted in South Florida to date.

International Cyber Crime Trends

The Global nature of the Internet enables Cyber criminals the low cost opportunity to target victims from countries that previously might have been out of reach.

Although initially established to support domestic law enforcement efforts, the Internet Crime Complaint Center (IC3) continues to receive an increasing number of complaints from victims outside the U.S. These complaints have also identified the perpetrators of such acts as emanating from over 110 foreign countries.

Each complaint is forwarded to law enforcement for follow up action, varying degrees of success, and in many cases frustration, has been experienced in certain countries. Historically, one such country has been Nigeria.

The IC3 has received numerous complaints regarding Cyber crime activity allegedly originating from Nigeria. In recognition of the increasing Cyber threat associated with Nigeria, the IC3 together with Legat Lagos, Nigeria provided the details of the perpetrators' various on-line fraudulent criminal activities to their counterparts at the newly created Nigerian Economic and Financial Crimes Commission (EFCC). The EFCC expressed a serious interest and commitment to providing the necessary resources to address the ever growing on-line Nigerian criminal activity. Although the EFCC expressed a sincere interest in responding to Cyber crime matters, they also noted that they lacked the necessary skills and equipment to appropriately target the on-line criminal element. In response, and in order to support the Nigerian's in this new endeavor, the FBI provided computer crime investigation training to Nigerian law enforcement, and agreed to seek additional resources/training to further their capabilities.

The FBI and all United States law enforcement has benefited greatly from the investigative efforts of the EFCC. Recently, the FBI assigned an agent to work exclusively with the EFCC, as Nigerian law enforcement targeted the Nigerian subjects, who were some of the culprits behind the ever popular on-line fraudulent activity that is commonly referred to as the "Reshipper Scam." During that 30 day assignment, the EFCC conducted 14 controlled deliveries and arrested 17 subjects. The EFCC seized over $340,000 worth of fraudulently obtained on-line merchandise and recovered $115,000 in fraudulent cashier checks, which were issued against various United States financial institutions.

Within the last year, as a result of the efforts of the EFCC and FBI, Legat Lagos, 1 million dollars in fraudulently obtained on-line merchandise has been recovered in

To provide a better understanding of the newly created EFCC, the information noted infra was taken directly from the EFCC's website, www.efccnigeria.org:

Nigerian
Economic and Financial
Crimes Commission (EFCC)

INTRODUCTION

The preponderance of economic and financial crimes like Advance Fee Fraud (419), Money Laundering, etc has had severe negative consequences on Nigeria, including decreased Foreign Direct Investments in the country and tainting of Nigeria's national image. The menace of these crimes and the recognition of the magnitude and gravity of the situation led to the establishment of the Economic and Financial Crimes Commission. The legal instrument backing the Commission is the attached EFCC (Establishment) Act 2002 and the Commission has high-level support from the Presidency, the Legislature and key security and law enforcement agencies in Nigeria.

THE EFCC (ESTABLISHMENT) ACT 2002

The Act mandates the EFCC to combat financial and economic crimes. The Commission is empowered to prevent, investigate, prosecute and penalize economic and financial crimes and is charged with the responsibility of enforcing the provisions of other laws and regulations relating to economic and financial crimes, including:

- The Money Laundering Act 1995
- The Advance Fee Fraud and Other Fraud Related Offences Act 1995
- The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994
- The Banks and other Financial Institutions Act 1991; and
- Miscellaneous Offences Act

In addition, the EFCC will be the key agency of government responsible for fighting terrorism.

Significance of the EFCC

The EFCC strives to combat economic and financial crimes through the establishment of cooperative working relationship with established enforcement and regulatory to achieve a flourishing economy where industry, hard work and dedication to duty remain the yardstick for measuring success rather than the existing recognition of ill gotten wealth through criminal activities.
This will be achieved through the use of highly skilled professional and motivated staff who will identify and trace offenders, and also be engaged in data collection, investigations and the seizure of the assets of criminal enterprises both domestically and internationally with the assistance of similar international agencies.

EFCC Mission Statement

The EFCC will;

- Curb the menace of corruption that constitutes the cog in the wheel of progress;
- Protect national and foreign investments in the country;
- Imbue the spirit off hard work in the citizenry and discourage ill gotten wealth;
- Identify illegally acquired wealth and confiscate it
- Build an upright workforce in both public and private sectors of the economy and;
- Contribute to the global war against financial crimes.

Old Scheme, New Twist

In July 2004, the Internet Crime Complaint Center (IC3), received information indicating that the notorious Nigerian email/letter scam had taken an ominous transformation from the traditional advance fee scheme to extortion with a threat of physical violence.

After receiving this information, the IC3 forwarded this new intelligence to the Nigerian Economic and Financial Crimes Commission (EFCC). Subsequently, the EFCC informed the IC3 that, based on the information previously provided by the IC3; one subject was arrested as he attempted to withdraw funds from the bank account that was listed in the extortion email.

Following is an ***exact*** copy of the email IC3 provided the EFCC:

From: Secretary Towogbola [secretary_in_chargeeeee@hotmail.com]
Subject: TREAT AS URGENT {THIS IS NO JUNK MAIL}

"EXECUTION"EXECUTION"EXECUTION"'
NATIONAL CORPORATION HEADQUATERS LAGOS.

PRIVACY. we wish to introduce our company/ourselves as a subsidiary of INTERNATIONAL ASSASINATORS AND WORLD SECURITY ORGANISATIONS, with branches in one hundred and two {102}countires.

we have received a fax message from our headquaters,new york,this morning to inform you to produce a mandatory sum of US$40,000.00 {FOURTHY THOUSAND UNITED STATES DOLLARS} only,into our account given below in nigeria within ninety six hours{96},alternatively you will be SNIPPED and GUNNED down during the period of our oncoming anniversary of fifty years.

STANDARD TRUST BANK VICTORIA ISLAND BRANCH LAGOS A/C NO. 03681173101152 {OLAJIDE .O. WILLIAMS} NIGERIA

CAUTION.

1.you are to attach and send with immediate effect,the payment slip,confirming the payment and to enable us to reconcile with our files and deploy our men already monitoring you.

2.we will as well waste no time to carry our operations,if we discover that this contact is disclosed to any second party including the following:-

{a}police {b}relation and {c}friends

3.we guarantee your saftey locally and internationally,on the completion of this contract and will not hesitate to disclose our men in your country to you and as well render our service if needed or on request.

we seek your urgent co-operation,for it is not our wish to get you eliminated.

Note : - Your death has been paid for by someone you offended sometime ago and it will be adviceable that you co-operate with us a.s.a.p.

TOWOGBOLA .A.JOHNSON SECRETARY.

Romanian Efforts

International progress is being made in the arena of Cyber investigations supported by partnerships established by the FBI at the Internet Crime Complaint Center (IC3). These partnerships include the Legal Attache (Legat) Program, private industry,

and the international law enforcement community. The following investigation illustrates a recent example of how these partnerships help to advance a significant international Cyber crime case to a successful conclusion.

In September of 2003, the IC3 began working with the Directorate for Combating Organized Crime and Antidrug (DGCCOA), Ministry of the Interior, Romania, a central Romanian law enforcement agency in Bucharest, Romania. The DGCCOA had developed a case regarding subjects Paul Gruia and Paraschiv Marius Cornel. Gruia and Cornel are brothers who posted fraudulent Internet auctions from Romania, purporting to sell expensive electronic items, and collecting advanced payments via wire transfer. This matter originally identified a potential group of subjects targeting a small number of U.S citizens. In collaborative efforts between the DGCCOA, IC3, and industry, the initial group of victims was quickly expanded to include more than 100 victims and losses exceeding $60,000. On July 14, 2004, the DGCCOA arrested subjects Paraschiv Marius Cornel, Gruia Paul, Maftei Razvan Gabriel, and Radu Ciprian.

In one of the largest computer intrusion/Internet fraud investigations ever, an FBI investigation in Los Angeles, other FBI field offices across the country, and international law enforcement authorities yielded an August 2004 federal grand jury indictment of a Romanian computer hacker and five Americans on charges that they conspired to steal more than $10 million in computer equipment from Ingram Micro in Santa Ana, California, the largest technology distributor in the world.

The indictment alleges that Calin Mateias hacked into Ingram Micro's online ordering system and placed fraudulent orders for computers and computer equipment. He directed that the equipment be sent to dozens of addresses scattered throughout the United States as part of an Internet fraud ring.

The 14-count indictment charges:

• Mateias, 24, of Bucharest, Romania, who used the online nickname "Dr. Mengele";
• Olufemi Tinubu, 21, of Atlanta;
• Tarion Finley, 20, also of Atlanta;
• Valeriu Crisovan, 27, of Hallandale, Florida;
• Jeremy Long, 28, of Richmond, Virginia; and
• Warren Bailey, 21, of Anchorage, Alaska.

The five defendants in the United States will be ordered to appear in United States District Court in Los Angeles for arraignment later this month. The Justice Department is working closely with Romanian authorities to ensure that Mateias is brought to justice, whether in Romania or the United States.

According to the indictment, Mateias began hacking into Ingram Micro's online ordering system in 1999. Using information obtained from his illegal hacking activity, Mateias bypassed Ingram's online security safeguards, posed as legitimate customers and ordered computer equipment to be sent to Romania. When Ingram Micro blocked all shipments to the Eastern European country in early 1999, Mateias recruited Tinubu, Crisovan, Long and Bailey from Internet chat rooms to provide him with United States addresses to use as "mail drops" for the fraudulently ordered equipment. Crisovan, Tinubu, Finley and Long, in turn, recruited others, including high school students, to provide additional addresses and to accept the stolen merchandise. The defendants in the United States would either sell the equipment and send the proceeds to Mateias, or they would repackage the equipment and send it to Romania.

Mateias and his co-conspirators allegedly fraudulently ordered more than $10 million in computer equipment from Ingram Micro. However, Ingram Micro was successful in intercepting nearly half the orders before the items were shipped.

All six defendants are charged with conspiring to commit mail fraud by causing Ingram Micro to ship computer equipment based on the false pretenses that the equipment was ordered by legitimate customers. In addition to the conspiracy count, Mateias is charged with 13 mail fraud counts; Tinubu and Finley are charged with three mail fraud counts; Crisovan is charged with six mail fraud counts; and Long is charged with four mail fraud counts for shipments.

Identity Theft

In February 2001, an investigation was initiated into the activities of a large Eastern European organized crime group. The organized crime group executed a variety of schemes to defraud U.S. consumers, merchants, and banks. The principal scheme involved "web phishing" activities aimed at deceiving consumers into disclosing their credit card numbers and other sensitive information. The group then used the stolen credit card numbers to purchase merchandise over the Internet.

In order to execute this scheme, the suspects recruited individuals in the U.S. to receive merchandise and money on their behalf. The recruited individuals were directed to reship the merchandise to individuals in Eastern Europe. The recruited individuals were also instructed to deposit the money into their bank accounts and forward the money to other accounts in the U.S. and overseas to be laundered.

There have been approximately 30 arrests to date related to this organized crime group. The most recent arrest occurred on June 4, 2004, in Leeds, Great Britain, when the National High Tech Crime Unit (NHTCU) from Great Britain arrested a high-level member of the organization, who is known to be responsible for the organization's

money laundering operation. The NHTCU charged the defendant with possession of a firearm and two counts of possession of fraudulent documents. UK investigators also initiated a search of his residence and seized large quantities of cash, laptops, fraudulent IDs, and forging equipment.

U.S. Postal Inspectors worked closely with the Department of Justice Computer Crime Intellectual Property Section (CCIPS), and its task force, in identifying and locating the defendant arrested on June 4, 2004. This case is being investigated by the CCIPS, U.S. Postal Inspection Service, FBI, U.S. Secret Service, Internal Revenue Service – Criminal Investigations Division, and the Drug Enforcement Agency.

Agencies participating in the Web Snare initiative include:

Albemarle County Police Department, Charlottesville, Virginia
Albemarle Sheriff's Office, Albemarle, Virginia
Anne Arundel County Police Department, Annapolis, Maryland
Arlington Heights Police Department, Chicago, Illinois
Bacau, Romania Police
Baltimore City Police Department, Baltimore, Maryland
Bellingham Police Department, Bellingham, Washington
Bridgeton Police Department, Bridgeton, New Jersey
Bureau of Immigration and Customs Enforcement
Central Ohio Cybercrime Task Force
Chesterfield Police Department, Chesterfield, Missouri
Chula Vista Police Department, Chula Vista, California
Culpeper Sheriff's Office, Culpeper, Virginia
Dallas Police Department, Dallas, Texas
Department of Defense
Department of Energy, Office of Inspector General
Department of Justice, Computer Crime Intellectual Property Section
Department of Motor Vehicles, California
Department of Transportation, Office of Inspector General
Directorate for Combating Organized Crime and Anti-Drug, Romania
Ebay Fraud Investigation Unit, San Jose, California
Erath County District Attorney, Stephenville, Texas
Erie County Sheriff's Office, Buffalo, New York
Fairfax County Police Department, Fairfax, Virginia
Fairmont City Police Department, Fairmont, West Virginia
Fayette County Prosecuting Attorney's Office, Fayetteville, West Virginia
Fayette County Sheriff's Office, Fayetteville, West Virginia
Federal Bureau of Investigation
Federal Trade Commission
Ghanaian Law Enforcement Officials
Gresham Police Department, Gresham, Oregon
Hanover County Sheriff's Office, Hanover, Virginia
Harris County District Attorney's Office, Consumer Fraud Division

Internal Revenue Service
Johnson County Sheriff's Office, Warrensburg, Missouri
Kentucky Attorney General's Office
Las Vegas Metro Police Department, Las Vegas, Nevada
Louisville Metro Police Department, Louisville, Kentucky
Matteson Police Department, Matteson, Illinois
Miami Township Police Department, Clearmont County, Ohio
Michigan State Police
Mid-Michigan Area Computer Crimes Task Force
Monmouth County Prosecutor's Office, Freehold, New Jersey
Mt. Hope Police Department, Mt. Hope, West Virginia
National Aeronautics and Space Administration, Office of Inspector General
National Hi-Tech Crime Unit
Nevada Cyber Crime Task Force
Nevada State Attorney General's Office
Newport News Police Department, Newport News, Virginia
Newton Police Department, Newton, Kansas
New York State Police
Niagara Frontier Transportation Authority Police Department, Canada
Norman Police Department, Cleveland County, Ohio
Northern California Computer Crimes Task Force, Napa, California
Northwest Cyber Crimes Task Force, Seattle, Washington
Oak Hill Police Department, Oak Hill, West Virginia
Office of the State's Attorney for Anne Arundel County, Annapolis, Maryland
Oklahoma Attorney General, Oklahoma City, Oklahoma
Oregon City Police Department, Oregon City, Oregon
Peel Regional Police Department, Ontario, Canada
Pennsylvania State Police
Perry Township Police Department, Massillon, Ohio
Provincial Weapons Enforcement Unit, Ontario, Canada
Richardson Police Department, Richardson, Texas
Romanian National Police
Royal Canadian Mounted Police
Sacramento County Sheriffs Department, Sacramento, California
Sacramento Valley High-Tech Task Force
Saginaw County Sheriff's Office, Saginaw Michigan
San Diego Police Department, San Diego, California
San Diego Sheriff's Office, San Diego, California
San Jose Police Department, San Jose, California
Seattle Police Department, Seattle, Washington
Social Security Administration
South Bay High Tech Crimes Unit, California
St. Charles County Sheriff's Department, St. Charles, Missouri
St. Petersburg Police Department, St. Petersburg, Florida
Stephenville Police Department, Stephenville, Texas
Terrebonne Parish Sheriff's Office, Houma, Louisiana

Texas Office of the Attorney General, Austin, Texas
Trident Drug Task Force, West Virginia
United States Air Force, Office of Special Investigations
United States Attorney's Office
United States Bureau of Immigration and Customs Enforcement
United States Marshals Service
United States Navy, Criminal Investigative Service
United States Postal Inspection Service
United States Secret Service
United States Securities and Exchange Commission
Utah Cybercrimes Task Force
Virginia Attorney General's Office
Warren Police Department, Warren, Michigan
Wausau Police Department, Wausau, Wisconsin
West Virginia State Police, Fairmont, West Virginia
Whatcom County Sheriff's Office, Bellingham, Washington

Consumer Tips for Phishing Attacks

The number and sophistication of phishing scams sent to consumers within the last year has increased dramatically. While online banking and e-commerce is, as a general rule, very safe, caution must be exercised before giving out personal financial information over the Internet. The Anti-Phishing Working Group has compiled the following list of recommendations that you can use to avoid becoming a victim of these scams:

- Be suspicious of any email with urgent requests for personal financial information
  - unless the email is digitally signed, you can't be sure it wasn't forged or "spoofed"
  - phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
  - phishers typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
  - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
  - instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
- Avoid filling out forms in email messages that ask for personal financial information
  - you should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
  - to make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"
- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites
  - EarthLink ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites.
  - Its free to all Internet users - download at http://www.earthlink.net/earthlinktoolbar
- Regularly log into your online accounts
  - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
  - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
  - in particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page --

http://www.microsoft.com/security/ -- to download a special patch relating to certain phishing schemes

- Always report "phishing" or “spoofed” e-mails to the following groups:
  - forward the email to reportphishing@antiphishing.com
  - forward the email to the Federal Trade Commission at spam@uce.gov
  - forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
  - notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/
  - when forwarding spoofed messages, always include the entire original email with its original header information intact

CAN SPAM Act
Quick Reference Guide

Controlling the **A**ssault of **N**on-**S**olicited **P**ornography **A**nd **M**arketing

- Legislation drafted with input from ISPs, email marketers, DOJ, etc.
- Has both civil and criminal remedies
- Effective on January 1, 2004

Civil Provisions

- *Opt-out* scheme overall
- Civil enforcement for:
    - False or misleading routing headers
    - Deceptive subject lines
    - Failure to include return address for opt-out
    - Sending email after objection
    - Failure to include indication that is solicitation
    - Unmarked sexually explicit spam
- FTC, State AGs, and ISPs may sue for violations
    - *No private right of action* by individual recipients

Criminal Provisions

- Fraudulent Spam
    - CAN-SPAM establishes 18 U.S.C. § 1037, with criminal penalties for five types of activities
    - Key phrase for spam is "*multiple commercial electronic mail messages*"
    - "Multiple" means more than:
        - 100 messages in 24 hours
        - 1,000 messages in 30 days
        - 10,000 messages in 1 year
    - For criminal provisions, messages need not be *unsolicited,* but must be *commercial.*
        - "Primary purpose" must be advertising
    - Conspiracy to undertake activity included as an offense

Pornographic Spam

- Section 5(d) (codified at 15 U.S.C. § 7704(d)) requires labels on spam containing "sexually oriented material":
    - FTC assigned duty to prescribe marks required to be included
    - Content of email available when opened can be no more than governmentally-required material on initial opening of mail
    - Civil penalties applicable to violations
    - Additionally, paragraph (d)(5) provides that "[w]hoever knowingly violates paragraph (1)" shall be punished by up to five years imprisonment

Five Types of Spam

- 1037(a)(1) -- Hacking to Spam

"Whoever, in or affecting interstate or foreign commerce, knowingly…accesses a protected computer without authorization and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer…"

  - Activity may also be covered by 18 U.S.C. § 1030
  - Automatically receives higher penalty (3 years)

- 1037(a)(2) -- Using Relaying to Deceive

"Whoever, in or affecting…commerce, knowingly…uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages…"

  - Specific intent provision designed to protect against innocent uses of relays

- 1037(a)(3) -- False Header Information

"Whoever, in or affecting…commerce, knowingly…materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages…."

  - Materiality standard applies here:
  - Information is materially falsified if it is altered or concealed in a manner that would impair the ability recipients, ISPs, or law enforcement to identify, locate, or respond to the person who initiated the message

- 1037(a)(4) -- Anonymous Email Abuse

"Whoever, in or affecting… commerce, knowingly…registers, using information that materially falsifies the identity of the actual registrant, for 5 or more electronic mail accounts or online user accounts or 2 or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names…"

- 1037(a)(5) -- Zombie Spam

"Whoever, in or affecting… commerce, knowingly…falsely represents oneself to be the registrant or legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses…"

Penalty

- 5 years if either apply:
  - Committed in furtherance of a felony under federal or state law
  - Defendant previously convicted under §§ 1030 or 1037 or a state law for conduct involving spam or unauthorized access to a computer system
- 3 years if any apply:
  - Hacking to spam ((a)(1) Offense)
  - Account registration ((a)(4)) offense that involved 20 or more email accounts or 10 or more domains
  - Volume exceeded 2,500 per day, 25,000 per month, or 250,000 per year
  - Offense caused loss of $5,000 or more in a year
  - Perpetrator gained $5,000 or more in value in a year

    - Perpetrator was organizer or leader of three or more others
- Otherwise, one year misdemeanor

Sentencing Guidelines and Forfeiture

- Sentencing Commission directed to issue guidelines considering enhancements for:
    - Dictionary attacks and address harvesting
    - Knowing use of domains with false registration information
    - Using spam to facilitate other crimes
- Criminal Forfeiture available for:
    - Any property traceable to gross proceeds of offense
    - Any equipment, software, etc. used or intended to be used in commission of the offense

CONSUMER AND BUSINESS EDUCATION MATERIALS

The following materials can help consumers avoid the scams practiced in these cases and advise businesses on how to comply with the CAN-SPAM Act. (The links listed are for the text versions, but by changing the ".htm" to ".pdf", you can link to the pdf files of the same materials.)

The CAN-SPAM Act: Requirements for Commercial Emailers
http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm

Ready to Pop Your Top Over "Pop Up Spam?" Here's How to Make it Stop
http://www.ftc.gov/bcp/conline/pubs/alerts/popalrt.htm

Diversity Visa Lottery: Read the Rules, Avoid the Rip-Offs
http://www.ftc.gov/bcp/conline/pubs/alerts/lottery.htm

How Not to Get Hooked by a 'Phishing' Scam
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

Looking for the Best Mortgage
http://www.ftc.gov/bcp/conline/pubs/homes/bestmorg.htm

Statement By Ken A. Wasch, President,
Software & Information Industry Association

WASHINGTON, D.C. – August 26, 2004 – In response to the FBI's announcement on Web-Snare, the Bureau's latest software piracy sting operation, Ken Wasch, President of the Software & Information Industry Association (SIIA), issued the following comments:

"SIIA commends the U.S. Government on their continuing efforts to combat online piracy. The Department of Justice's involvement in the fight against theft of digital code and content is integral to successfully eradicating this type of criminal activity."

"Offenders believe that the act of digital piracy is a victimless crime that goes unpunished. It is essential to send a clear message to digital pirates that stealing copyrighted works is illegal and can result in stiff fines and even jail time. The action announced today – in conjunction with prior enforcement activities – underscores that message."

"SIIA will continue to support law enforcement agencies in their efforts to protect copyrighted works and eliminate Internet crime."

About SIIA

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital content industry. SIIA provides global services in government relations, business development, corporate education and intellectual property protection to more than 600 leading software and information companies. For further information, visit http://www.siia.net.

# # # #

MOTION PICTURE ASSOCIATION OF AMERICA, INC.
15503 VENTURA BOULEVARD
ENCINO, CALIFORNIA 91436

August 20, 2004

Robert S. Mueller III
Director
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

RE: OPERATION WEB SNARE

Dear Director Mueller:

The Motion Picture Association of America (MPAA) wishes to thank you, the Federal Bureau of Investigation, and the Internet Crime Complaint Center for your outstanding work in connection with Operation Web Snare. Operation Web Snare evidences a law enforcement commitment to combating intellectual property crime that is desperately needed in the war against pirates who drain the life blood of our industry. We are extremely grateful to you, the Federal Bureau of Investigation, and the Internet Crime Complaint Center for your leadership roles in addressing the serious threats to the movie industry posed by these thieves.

We estimate that the U.S. motion picture industry loses in excess of $3 billion annually in potential worldwide revenue due to piracy. Pirate activities undermine every aspect of the legitimate

filmmaking business since legitimate retailers cannot possibly compete fairly with pirate businesses. We hope that Operation Web Snare will send a strong message to pirates that stealing intellectual property is a serious crime that carries with it serious consequences. Piracy is not a victimless crime, and we wish to thank you for your commitment to fighting such crime with the actions announced today.

Sincerely,

James W. Spertus
Vice President and Director
United States
Anti-Piracy Operations

About the MPAA:

The Motion Picture Association of America, Inc. (MPAA) serves as the voice and advocate of the American motion picture, home video and television industries from its offices in Los Angeles and Washington, D.C. These members include: Buena Vista Pictures Distribution; Metro-Goldwyn-Mayer Studios Inc.; Paramount Pictures; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal Studios from Universal City Studios; and Warner Bros. Entertainment Inc.

Statement by Robert Holleyman

President and CEO, Business Software Alliance

The Business Software Alliance (BSA), an industry watchdog for the software industry, applauds the recent action taken by the FBI in Web-Snare.

BSA has seen an increase in law enforcement activity aimed at combating criminal software piracy on the Internet. We commend the FBI for its leadership and initiative in addressing the serious threat of software piracy. Globally, piracy impacts software publishers and consumers and costs the industry nearly $29 billion worldwide annually.

We hope that law enforcement agencies' increased attention to this problem will send the message that piracy is often a crime that can result in very serious consequences. BSA hopes that if the consequences of engaging in copyright infringement over the Internet continue to become known, there will be less of a need for future criminal prosecutions.

The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CNC Software/Mastercam, Internet Security Systems, Macromedia, Microsoft, McAfee, SolidWorks, Sybase, Symantec, UGS and VERITAS Software.

August 20, 2004

Director Robert Mueller:

The Merchant Risk Council is pleased to continue working with Law Enforcement and we are very pleased to establish formal partnerships with the Internet Crime Complaint Center, FBI, and other areas of law enforcement.

Through collaboration with law enforcement we firmly believe our organization is helping ensure that on-line shopping continues to be safe and profitable for both consumers and merchants.

Julie Fergerson
Co-Chair, Merchant Risk Council
512-977-5525

About the Merchant Risk Council

The Merchant Risk Council (formerly known as the Merchant Fraud Squad) is a not-for-profit organization founded in September 2000. It provides education about fraud prevention techniques and encourages businesses selling online to adopt best practices and anti-fraud technologies. The Network's merchant focus distinguishes this group from others that are trying to combat this problem.

To learn more about the Network and sign up to join, visit www.merchantriskcouncil.org.

Direct Marketing Association, Inc.
1120 Avenue of the America
New York, New York 10036–6700
Tel: 212.768.7277 Ext. 1704
Cell: 917.295.0121
Fax: 212.768.7353
E-Mail: bwientzen@the-dma.org

H. Robert Wientzen
President Emeritus

August 26, 2004

The Honorable John Ashcroft
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear General Ashcroft:

I want to thank you for your commitment to fight cybercrime, especially the fight against spam through the unique public/private-sector partnership, Operation SLAM Spam.

The Direct Marketing Association (The DMA) and its nearly 4,700-member companies, who are engaged in all facets of e-commerce and direct and interactive marketing, are extremely supportive of collaborative law enforcement operations targeting cybercrime. We look forward to continuing to participate in Operation SLAM Spam, in the expectation that The DMA's and the FBI's resources and expertise will bring about a safer and more trustworthy online environment for consumers and legitimate marketers alike.

The DMA has long advocated that strong and visible law enforcement, aided by the new and very strong provisions of the CAN-SPAM Act, will be one of the major deterrents to spammers. We continue to support vigorous enforcement of the law as a means to protect consumers and to preserve the continued growth of legitimate e-commerce.

The DMA and its members have done more than vocally support your efforts. As you may know, by initiating Operation SLAM Spam and supporting it financially, The DMA has been assisting in the FBI's ambitious efforts to identify and facilitate the prosecution of egregious spammers.

We praise the FBI for their willingness to join with The DMA and the e-commerce industry on this groundbreaking law enforcement effort. We are confident that Operation SLAM Spam will go a long way to stop those who are sending spam.

Finally, we also acknowledge the critical work of Senators McCain, Burns, Wyden and all of the members of the Senate Commerce and Judiciary Committees who were instrumental in passing the CAN-SPAM Act and President Bush for quickly enacting it into law.

We have been working with the Operation SLAM Spam team, the FBI, and others for over a year now, and applaud their ongoing interest and leadership in not only fighting spam, but in preserving the promise of e-mail as a powerful and efficient vehicle for global commerce, communication, and education.

Again, I thank you for your continued support of unique programs like Operation SLAM Spam and look forward to continuing our partnership into the future.

Sincerely,